UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/921,536	08/03/2001	John R. McGarvey	5577-236	6803

20792 7590 02/17/2005

MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 02/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/921,536	MCGARVEY ET AL.	
	Examiner	Art Unit	
	Matthew T Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 August 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☒ Claim(s) *5-22* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *8/3/2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

This action is in response to the communication filed on 08/03/2001.

DETAILED ACTION

1. Claims 1-32 have been examined.

Title

2. The title of the invention is acceptable.

Priority

3. No claim for priority has been made for this application.

4. The effective filing date for the subject matter defined in the pending claims in this application is 08/03/2001.

Information Disclosure Statement

5. The information disclosure statement (IDS) submitted on 08/03/2001 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

Drawings

6. The drawings filed on 08/03/2001 are acceptable for examination proceedings.

Specification

7. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

8. The abstract of the disclosure is objected to because

Line 1: The phrase "Methods, systems...provide for" can be implied and therefore must be removed.

Correction is required. See MPEP § 608.01(b).

Lines 3-4: The phrase "and the common nonce to the client" does not make sense and therefore must be removed or corrected.

Claim Objections

9. Claims 5-22 are objected to for failing to comply with the numbering standard as set forth in 37 CFR 1.75(c).

10. The applicant is reminded that a series of singular dependent claims is permissible in which a dependent claim refers to a preceding claim which, in turn, refers to another preceding claim.

A claim which depends from a dependent claim should not be separated by any claim which does not also depend from said dependent claim. It should be kept in mind that a dependent claim may refer to any preceding independent claim. In general, applicant's sequence will not be changed. See MPEP § 608.01(n).

Claim Rejections - 35 USC § 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United

States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

12. Claims 28, and 31-32 are rejected under 35 U.S.C. 102(e) as being anticipated by Ford (US Patent Number 6,829,356).

13. Regarding claim 28, Ford disclosed a method of authenticating a client, comprising: receiving at a server of a plurality of servers, a common nonce which is associated with each of the plurality of servers, the common nonce being signed by the client (See Ford Col. 15 Lines 56-61); and authenticating the client based on the received signed common nonce (See Ford Col. 15 Lines 61-65).

14. Claims 31-32 are rejected for the same reasons as claim 28 above, and further because Ford disclosed the system computer program product for doing the same (See Ford Claims).

Claim Rejections - 35 USC § 103

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

16. Claims 1-3, 5, 7-11, 14-15, and 26-27, and 29-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ford and further in view of Blakley, III et al. (US Patent Number 6,067,623) hereinafter referred to as Blakley.

17. Regarding claim 1, Ford disclosed a method for authenticating a client to a plurality of servers comprising: obtaining a common nonce associated with each of the plurality of servers (See Ford Col. 15 Lines 24-31); providing the common nonce to the client (See Ford Col. 15 Lines 56-61); and providing the signed common nonce as a signature for transactions from the client to the plurality of servers so as to authenticate the client to the plurality of servers (See Ford Col. 15 Lines 55-65). However, Ford failed to disclose a middle-tier server receiving the signed common nonce and providing the signed common nonce to the servers.

Blakley teaches that in a client to multiple server authentication system, providing a middle-tier server in the system, for receiving authentication information from the client and forwarding the information to each server, can reduce client to server traffic (See Blakley Abstract and Col. 1 Lines 43-67 and Col. 3 Paragraph 2).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Blakley in the authentication system of Ford by providing a middle-tier server for receiving the nonce challenges from the servers and sending them to the client, and for receiving the signed nonce message and providing the signed nonce message to the servers. This would have been obvious because the ordinary person skilled in the art would have been motivated to reduce the network traffic between the client and the servers.

18. Regarding claim 2, the combination of Ford and Blakley disclosed that the step of obtaining a common nonce comprises the step of generating a common nonce based on information obtained from each of the plurality of servers (See Ford Col. 15 Lines 56-61).

19. Regarding claim 3, the combination of Ford and Blakley disclosed that the step of generating a common nonce comprises the steps of: obtaining pre-nonce contributions from the

plurality of servers (See Ford Col. 15 Lines 24-31); combining the pre-nonce contributions to provide a single pre-nonce token; and providing the common nonce based on the pre-nonce token (See Ford Col. 15 Lines 56-61 wherein it was inherent that the nonce challenges were combined in order for the client to have had the nonce message).

20. Regarding claim 5, the combination of Ford and Blakley disclosed that the step of combining the pre- nonce contributions to provide a single pre-nonce token comprises concatenating the pre-nonce contributions (See Ford Col. 15 Lines 56-61).

21. Regarding claim 7, the combination of Ford and Blakley disclosed that the step of obtaining pre-nonce contributions comprises the steps of: requesting a pre-nonce contribution from each of the plurality of servers (See Ford Col. 15 Paragraph 2); and receiving the pre-nonce contributions from the plurality of servers (See Ford Col. 15 Paragraph 2).

22. Regarding claim 8, the combination of Ford and Blakley disclosed that requesting a pre-nonce contribution comprises sending authenticated requests to the plurality of servers (See Ford Col. 15 Lines 1-22).

23. Regarding claim 9, the combination of Ford and Blakley disclosed the step of encrypting the authenticated requests sent to the plurality of servers (See Col. 15 Paragraph 1).

24. Regarding claim 10, the combination of Ford and Blakley disclosed that the authenticated requests include at least one of an identification of a source of the request, a time stamp and a random number (See Ford Col. 14 Paragraph 6 and Col. 15 Paragraph 1).

25. Regarding claim 11, the combination of Ford and Blakley disclosed that the pre-nonce contributions include at least one of an identification of a server of the plurality of servers and a random number (See Ford Col. 15 Lines 24-38, and Line 56 Col. 16 Line 2).

26. Regarding claim 14, the combination of Ford and Blakley disclosed the steps of: receiving a transaction identification from a trusted server of the plurality of servers; and associating the transaction identification with the common nonce (See Ford Col. 15 Lines 22-31).

27. Regarding claim 15, the combination of Ford and Blakley disclosed the step of tracking use of the common nonce based on the transaction identification (See Ford Col. 15 Line 22 - Col. 16 Line 2).

28. Regarding claim 26, see the rejection of claim 1 above.

29. Regarding claim 27, see the rejection of claim 1 above, and further the claims of Ford wherein a computer program product was disclosed.

30. Regarding claim 29, the combination of Ford and Blakley disclosed that a trusted third party provided the common nonce (See the rejection of claim 1 above, wherein the middle-tier server provided the nonce challenges/common nonce to the client after receiving the nonce challenges from the plurality of servers).

31. Regarding claim 30, the combination of Ford and Blakley disclosed that the common nonce was generated based on information provided by each of the plurality of servers.

32. Claims 4, 6, 12-13 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Ford and Blakley as applied to claim 3 above, and further in view of Schneier (Applied Cryptography).

33. Regarding claim 4, the combination of Ford and Blakley disclosed providing a common nonce (See Ford Col. 15 Lines 56-61), but failed to disclose reducing the nonce challenges to

provide the common nonce. However, Ford and Blakley did disclose digitally signing a message containing the nonce challenges (See Ford Col. 15 Lines 56-61).

Schneier teaches that when digitally signing a message, it is practical to hash the message and encrypt the hash, with a private key, as the signature, rather than encrypting the whole message (See Schneier Page 38 Section Signing Documents with Public-Key Cryptography and One-Way Hash Functions). Schneier also teaches that in such a system, to verify the signature, the verifier hashes the message, decrypts the signed hash with the signers public key, and verifies that the two hashes are the same (See Schneier Page 38 Section Signing Documents with Public-Key Cryptography and One-Way Hash Functions).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier in the digital signatures of Ford and Blakley by signing and verifying the hash of the nonce message instead of the whole nonce message. This would have been obvious because the ordinary person skilled in the art would have been motivated to increase the speed of the signing method.

34. Regarding claim 6, the combination of Ford, Blakley, and Schneier disclosed that the step of reducing the pre-nonce token to provide the common nonce comprises the step of hashing the pre-nonce token utilizing a one-way hash function so as to provide the common nonce (See the rejection of claim 4 above).

35. Regarding claim 20, the combination of Ford, Blakley, and Schneier disclosed that at least one of the plurality of servers carries out the steps of: receiving the signed common nonce, the common nonce and the pre-nonce token; hashing the received pre-nonce token; comparing the hashed pre-nonce token to the common nonce; indicating that the client is not authenticated if

the hashed pre-nonce token is different from the common nonce (See Ford Col. 15 Lines 56-65 and Schneier Page 38 Section Signing Documents with Public-Key Cryptography and One-Way Hash Functions).

36. Regarding claims 12-13, the combination of Ford and Blakley disclosed the client checking the nonce challenge from the server for requisite strength, and aborting the authentication process if the nonce challenge did not meet the requisite strength (See Col. 15 Lines 39-41), but failed to disclose that this check included checking the signature of the nonce challenge to verify that it was signed by the server.

Schneier teaches that digital signatures provide a means for verifying the sender of a message (See Schneier Page 37 Signing Documents with Public Key Cryptography).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier in the nonce challenge system of Ford and Blakley by having the server sign the challenges and having the client verify the signature of the challenges before using the challenges. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect against illicit alteration of the challenge nonce.

37. Claims 16-17, and 21-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Ford and Blakley as applied to claim 3 above, and further in view of Menezes et al. (Handbook of Applied Cryptography).

38. Regarding claim 21, the combination of Ford and Blakley disclosed the server receiving the nonce challenges, and authenticating the client based on whether the nonce challenges

included the nonce challenge of the server (See Ford Col. 15 Lines 56-65), but failed to disclose that the nonce challenges included random numbers.

Menezes teaches that nonce challenges can be random numbers (See Menezes Page 398).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Menezes in the nonce challenge system of Ford and Blakley by having the nonce challenges be random numbers. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide uniqueness and timeliness assurances in the system in order to avoid replay and interleaving attacks.

39. Regarding claims 16-17, and 22 the combination of Ford and Blakley disclosed a plurality of servers providing nonce challenges to a client in order to authenticate the client, and verifying the nonce in the response to the challenge (See Ford Col. 15) but failed to disclose giving the nonce an expiration time and further authenticating the client based on the expiration time.

Menezes teaches that when using nonce challenges the challenger should apply a timeout period to the nonce and not authenticate the client if the response is received after the timeout period has expired (See Menezes Page 398 Section (i).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Menezes in the nonce challenge system of Ford and Blakley by applying and checking a timeout period to the nonce when authenticating a client. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide protection against replay and interleaving attacks.

40. Claims 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Ford and Blakley, as applied to claim 3 above, and further in view of Menezes.

The combination of Ford and Blakley disclosed using a users public key to verify the signature of the nonce message by verifying that the signature corresponded to the signature of the clients private/public key pair (See Ford Col. 15 Lines 56-65), but failed to disclose that the verifying server got the public key from a public key certificate and also failed to disclose that the authentication would fail if the certificate was not trusted.

Menezes teaches that public key certificates are a means to store, distribute, and forward public keys without danger of undetectable manipulation. Menezes also teaches that when using a certificate for authentication, the certificate is received, the expiration date is checked, the certification authority validity is checked, the signature of the certificate is checked, and the certificate is checked to see if it has been revoked, and if these checks pass then the public key is valid (See Menezes Pages 559-560).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Menezes in the authentication system of Ford and Blakley by obtaining the public key from a public key certificate and verifying that the certificate is valid in order to use the public key to authenticate the client. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect against undetected manipulation of the public key.

41. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Ford and Blakley as applied to claim 1 above, and further in view of Day (US Patent Number 6,052,784).

The combination of Ford and Blakley disclosed a challenge nonce system (See Ford Col. 15) but failed to disclose the nonce being received from a trusted third party and verifying the signature of the trusted third party.

Day teaches that a nonce can be signed by a trusted third party in order to authenticate the nonce (See Day Col. 3 Paragraph 5).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Day in the nonce challenge system of Ford and Blakley by having the nonce challenges signed by a certification authority prior to sending the challenge to the client, and verifying the signature on the nonce. This would have been obvious because the ordinary person skilled in the art would have been motivated to prevent the nonce from being illicitly undetectably modified prior to the client receiving the nonce challenge.

42. Claims 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Ford, Blakley, and Day as applied to claim 23 above, and further in view of Menezes.

Claims 24-25 are rejected for the same reasons as claims 18-19 above, as applied to claim 23 above.

Conclusion

43. Claims 1-32 have been rejected.

44. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Brezak et al. (US Patent Application Publication 2002/0150253) disclosed a system in which a server authenticates a client and once authenticated the server presents authentication information to a plurality of servers.

b. Brezak et al. (US Patent Application Publication 2003/0018913) disclosed a system in which a server receives authentication information from a client and delegates the information to a plurality of other servers, the system involving a trusted third party to provide authentication of the client.

c. Bartolomeos et al. (PCT Publication WO 99/56194) disclosed a system in which a server authenticates a client and then provides authentication of the client to a plurality of other servers.

d. Damour et al. (European Patent Application EP1168763) disclosed a system in which a server authenticates a client using nonce challenges and then delegates the authorization to other servers.

45. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew Henning
Assistant Examiner
Art Unit 2131
2/15/2005

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER